

Approved For Release 2001/03/02 : CIA-RDP78-04007A001000030044-0

60 /

Approved For Release 2001/03/02 : CIA-RDP78-04007A001000030044-0

Approved For Release 2001/03/02 : CIA-RDP78-04007A001000030044-0

~~RESTRICTED~~

*F-5
true
as is
TOP*

SECURITY REGULATIONS

CENTRAL INTELLIGENCE GROUP

~~RESTRICTED~~

Approved For Release 2001/03/02 : CIA-RDP78-04007A001000030044-0

RESTRICTED

**CENTRAL INTELLIGENCE GROUP
SECURITY REGULATIONS**

RESTRICTED

RESTRICTED

**CENTRAL INTELLIGENCE GROUP
2430 E STREET NW.
WASHINGTON 25, D. C.**

15 August 1947

The security regulations and procedures contained herein will be complied with by all members of the Central Intelligence Group. It is imperative in the interest of national security that the security program of this organization be supported in every detail by each member of the Group, irrespective of position.

All security regulations and instructions heretofore issued are superseded by the provisions of this manual.

[Redacted]
R. H. Hillenkoetter
Rear Admiral, U. S. N.
Director, Central Intelligence Group

FOIAb3b

RESTRICTED

d. Recommendation of penalty.

4. a. Assistant Directors and Staff Chiefs will determine seriousness of offense and whether a penalty should be imposed, and will direct imposition of first and second violation penalties when appropriate.

b. Recommendation for imposition of third and fourth violation penalties, or dismissal for other than a fourth violation penalty, will be forwarded to the Personnel Officer, with all papers on the case concerned.

5. a. These instructions shall apply to personnel detailed to duty with CIA from other government agencies except that the relief of such an individual from duty with CIA and return to his parent agency will be recommended in lieu of suspension or termination of employment.

b. Such an individual may elect to request reference of his case to the agency from which detailed rather than accept the penalty prescribed by paragraphs 1a and b. In such a case a report of the circumstances will be forwarded through the Executive for reference to the appropriate agency.

6. Assistant Directors, Staff Chiefs and the Personnel Officer are charged with informing the Chief of Inspection and Security of findings and punitive action taken by them in connection with each security violation for which penalties are imposed under these regulations.

7. As an incentive toward security-mindedness in the individual, and in order to remove a burden from the individual who has clearly demonstrated that he is no longer a risk with respect to physical security matters, the following exceptions to paragraph 1 are directed:

a. If the first violation occurs on a date more than two years after an individual first enters on duty with CIA, the particular provisions of paragraph 1a(1) shall not be applied.

b. If an individual serves two continuous years without a security violation, any or all violations which he committed prior to the commencement of said two year period shall be stricken from the records, insofar as the application of this Administrative Instruction is concerned.

8. Assistant Directors and Staff Chiefs will inform their employees of their security records under this policy.

FOR THE DIRECTOR OF CENTRAL INTELLIGENCE:

25X1A9a

Captain, USN
Executive

CENTRAL INTELLIGENCE AGENCY
Washington, D. C.

ADMINISTRATIVE INSTRUCTION
NO. [REDACTED]

30 June 1949

SUBJECT: Security Violation Penalty System.

1. A guide for the imposition of penalties for violation of CIA security regulations is given below:

a. First Violation:

(1) Verbal reprimand by division or higher chief and warning of possible consequences of further violations.

(2) Security-check duty for one week under direction of the appropriate staff duty officer.

b. Second Violation:

(1) Written reprimand and warning by Assistant Director or Staff Chief.

(2) Security-check duty for two or more weeks under direction of the appropriate staff duty officer.

c. Third Violation:

(1) Suspension without pay for a period not less than one week and not more than four weeks.

(2) Written warning from the Personnel Officer as to consequences of a fourth violation.

d. Fourth Violation: Termination of employment with CIA.

2. The above guide will not be a bar to immediate termination of employment due to any security violation considered sufficiently serious to warrant such action.

3. Security violations will be reported in writing, by branch chiefs or officials holding similar supervisory positions, to the Assistant Director or Staff Chief concerned, including:

a. Name of offender and nature of violation.

b. Opinion as to seriousness, and whether carelessness or negligence were involved.

c. Statement by the offender.

RESTRICTED

**CENTRAL INTELLIGENCE GROUP
SECURITY REGULATIONS**

ALPHABETICAL INDEX

SUBJECT	PAGE
Abstracting of Classified Documents	13
Administrative Action, Non-Compliance With Secrecy Agreement and Security Regulations	3
Admittance to Buildings After Hours, Badge Holders	6
Admittance of CIG Employees and Other Government Personnel to CIG Buildings	4 to 6
Admittance of Visitors	6-7
Alternate Top Secret Control Officers	13-14
Announcement of Connection With CIG	2
Assistant Top Secret Control Officers	14
Authority to Determine Classification	9-10
Badges	4-6
Badges, Issuance of	5
Badge Limitations	5
Change of Status	4
Clearance For Users of Top Secret Material	14
Classification Adjustments	12-13
Classification, Authority to Determine	9-10
Classified Documents, Destruction of	11-12
Classified Documents, Duplicating or Abstracting of	13

RESTRICTED

RESTRICTED

Alphabetical Index (continued)

SUBJECT	PAGE
Classified Documents, Loss or Compromise of	12
Classified Documents, Security of	8 to 17
Classified Documents, Storage of	10
Classified Documents, Transmission of, Outside of CIG	15-16
Classified Documents, Transmission of, Within CIG	16-17
Classified Waste, Disposition of	11
Compromise of Classified Documents	12
Concept of Security	1
Court Proceedings, Arrests, Traffic Accidents	19
Credentials, Issuance of	5
Credit Reference, CIG	19
Declassification	12-13
Defective Storage Equipment	18
Definitions of Security Classifications	8-9
Destruction of Classified Documents	11-12
Discussion of CIG Activities	19
Disposition of Classified Waste	11
Dissemination of Classified Information, Restrictions on	12
Documents, Safekeeping of	10
Duplicating or Abstracting of Classified Documents	13
Escorts, Visitor	6-7
Exit Interview	4
Field Installations, Security of	20

RESTRICTED

RESTRICTED

Alphabetical Index (continued)

SUBJECT	PAGE
Forgotten Identification Credentials	6
General Security Practices	17 to 20
Guards	7-8
Identification Credentials	4 to 6
Indoctrination Class	3
Indoctrination, Security	3
Inter-Agency Office Personnel, Contact Branch, O.O.	5
Issuance of Badges or Special Credentials	5
Keys to Offices	8
Leave of Absence	4
Legal Action, Violation of Espionage Act	3
Limited Pass	5
Logs, Maintenance of	16
Loss or Compromise of Classified Documents	12
Lost Identification Badges	5
Maintenance of Logs	16
Marking of Material	10
Night Duty Officers, Security Only	20
Penalties for Non-Compliance, Secrecy Agreement, Security Regulations	2-3 ,12
Policy Governing Unofficial Publications and Related Matters	2
Policy Governing Use of Official Data	1
Preliminary Indoctrination	3
Processing of Employees for Entrance on Duty, Leaves of Absence and Separations	3-4

RESTRICTED

RESTRICTED

Alphabetical Index (continued)

SUBJECT	PAGE
Processing of Incoming TOP SECRET Documents	14-15
Publications and Utterances Relating to Intelligence	2
Publications and Utterances, Other Than Intelligence	2
Public Buildings Administration Maintenance Employees	5-6
Receptionist Staff	7
Registered Documents	9
Restricted Area, Signal Center	5
Restrictions on Dissemination of Classified Information	12
Safekeeping of Documents	10
Safes	10-11
Secrecy Agreement	3
Secrecy Agreement, Penalties for Non-Compliance	2-3, 12
Securing Office at End of Day	18-19
Security of Buildings and Installations	4 to 8
Security Check, Staff	19-20
Security Classifications, Definitions of	8-9
Security of Classified Documents	8 to 17
Security of Field Installations	20
Security Indoctrination	3
Security in Office Routine	17 to 19
Security Outside of Office	19
Security Practices, General	17 to 20
Security Regulations, Penalties for Non-Compliance	2-3, 12

RESTRICTED

RESTRICTED

Alphabetical Index (continued)

SUBJECT	PAGE
Signature Record and Cover Sheet, TOP SECRET Documents	15
Social Activities, Group	19
Staff Security Check	19-20
Storage of Classified Documents	10
Telephones	17-18
Termination of Employment or Leave of Absence	4
TOP SECRET Documents, Processing of Incoming	14-15
TOP SECRET Control Officer and Alternates	13-14
TOP SECRET Control Procedure	13-14
TOP SECRET Log	15
TOP SECRET Material, Clearance For Users of	14
Transmission of Classified Documents, Outside of CIG	15-16
Transmission of Classified Documents, Within CIG	16-17
Unoccupied Rooms	18
Upgrading of Security Classification	12-13
Visitors	6-7
Visitor Entrances	7
Visitor Escorts	6-7
Visitor Pass	6
Visits During Off Duty Hours	7

RESTRICTED

RESTRICTED

**CENTRAL INTELLIGENCE GROUP
SECURITY REGULATIONS**

I GENERAL

1. CONCEPT OF SECURITY

- a. Security, as applied to an intelligence organization, is defined as a condition which assures the safeguarding of valuable information and the protection of physical and human assets, the compromise of which might seriously impair the interest of the Nation. In the intelligence field, it is imperative that a true state of security exist in time of peace, as well as in time of war.
- b. Even a partial compromise of security represents a loss which never can be regained—the damage is done. To prevent such a contingency requires the complete and unfailing cooperation of each and every member of the Central Intelligence Group, irrespective of position. Any employee, through carelessness, negligence, or by relaxing his security vigilance, even temporarily, may cause vital information to fall into the hands of unfriendly interests who are always on the alert to take advantage of lapses. Aside from the potentially grave consequences which acts of this type may cause, much valuable documentary material assembled at the expense of great effort on the part of many members of this organization may be completely nullified. Therefore, it is the responsibility of each individual employee of the CIG to train himself in the perpetual and unrelenting observance of all elements of security. Effective security is largely a matter of habit, the habit of discretion and care which has become second nature through constant usage. It must be cultivated by all employees if our mission and objectives are to be fully realized.

2. POLICY GOVERNING USE OF OFFICIAL DATA

- a. All information received or compiled by the CIG is official data and is the property of the United States Government. No officer or employee has any property interest in such information. The restrictions and prohibitions provided in this instruction apply not only to all intelligence information and material, but also to any statistical, administrative or general information, regardless of the fact that such information may already be a matter of general public knowledge. This shall also apply to all official data used or compiled by CIG and obtained from outside sources, public or private.

b. Official data are restricted to use in the performance of the official business of CIG and shall not be copied or removed from the files or from the premises of CIG except for official purposes.

c. No person connected with CIG in any official capacity shall accumulate copies of documents containing any such data for inclusion in a personal file, nor shall any person appropriate to his personal use, any official data acquired by virtue of his employment in CIG.

d. Exceptions to the regulations contained in this instruction will not be made except upon written approval of the Director of Central Intelligence. Authority to release official data shall be limited to officials designated by the Director of Central Intelligence.

RESTRICTED

RESTRICTED

2

3. POLICY GOVERNING UNOFFICIAL PUBLICATIONS AND RELATED MATTERS

The following policies are announced for the protection of CIG personnel in the interpretation of the various paragraphs of the Secrecy Agreement, upon the provisions of which, at their own willing acceptance, employment is conditioned. These policies are necessary in order to establish a procedure for clearance of public statements, releases to the press, official or unofficial publications, speeches or similar undertakings which might result in inadvertent disclosure of classified information. These policies are further necessary to preserve the confidential nature of employees' official positions and duties and to prevent inferences of official policy on the part of CIG in connection with national or international problems. The involvement of CIG employees in controversial matters of widespread importance may not only reveal official position and duties but may be construed as indicating CIG official policy.

a. *Publications and Utterances Relating to Intelligence*

Except by special direction or authorization in the name of the Director, no person employed by, or assigned to the Central Intelligence Group, shall teach a course, conduct a seminar, publicly make a speech or read a paper, or write for publication any material, the subject matter of which relates to intelligence or to the organization and functions of the CIG or other intelligence agencies.

b. *Other Publications, Activities and Utterances*

Clearances must be obtained by written application with respect to unofficial courses, addresses and publications believed to lie outside the prohibition set forth in subparagraph "a" above. Such applications shall enclose, in appropriate cases, the actual text of the proposed address or publication. Applications shall be addressed to the Director of Central Intelligence, through the appropriate Assistant Director and the Executive for Inspections and Security. Burden of proof that classified information will not be divulged rests with the applicant. Further, the applicant must establish that material to be publicized and the circumstances thereof do not involve controversial matter of national importance which might tend to disclose the author's official position and duties or appear to indicate by inference an official policy of CIG.

This paragraph does not apply to extemporaneous addresses arising from requests which would be embarrassing to refuse, so long as CIG personnel so called upon discuss subjects which are in no way allied to activities of the CIG, and so long as neither the speakers' connection with CIG nor the subject of intelligence, nor national policy matters are mentioned.

c. *Announcement of Connection with CIG*

In the event that clearance is granted under subparagraph "a" and "b" above, CIG personnel will not, under these circumstances, allow themselves to be presented, indicated or introduced as connected with CIG except by special authorization in the name of the Director.

4. PENALTIES FOR NONCOMPLIANCE

In accordance with paragraph 5 of the Secrecy Agreement, and inasmuch as employment by CIG is conditioned upon compliance with it and with these Security Regulations, any failure to observe these regulations, or a disregard thereof, will subject the employee or employees involved to immediate dismissal or to such disciplinary action as may be directed by the Director of Central Intelligence.

RESTRICTED

RESTRICTED

3

a. *Administrative Action*

In cases of noncompliance with CIG security requirements, the Director of Central Intelligence may take administrative action as follows: (1) separation, (2) suspension, (3) reprimand or (4) such other administrative action as shall be deemed advisable.

b. *Legal Action*

In cases of violation of the provisions of the Espionage Act (50 U.S.C. 31 and 32, as amended), employees are subject to criminal prosecution which may result in imprisonment for not more than ten years or a fine of not more than \$10,000, or both, at the discretion of the court.

II PROCESSING OF EMPLOYEES FOR ENTRANCE ON DUTY, LEAVES OF ABSENCE AND SEPARATIONS

5. SECRECY AGREEMENT

All personnel assigned to, or attached for duty with the Central Intelligence Group, prior to beginning their official duties will be required to execute a Secrecy Agreement which will be administered by the Director of Central Intelligence or his authorized representative.

6. SECURITY INDOCTRINATION

a. *Preliminary Indoctrination*

Subsequent to the receipt of security approval, and upon completion of all other necessary processing, the Personnel Branch will notify an applicant to report for duty. Prior to the time the employee actually commences his duties with the office to which he will be assigned, the Personnel Branch will instruct the employee to report to the Physical Security Branch, Executive for Inspection and Security, for Security Indoctrination and the issuance of a photographic building pass. Upon arrival at the Physical Security Branch, the individual will receive preliminary indoctrination and processing as follows:

(1) The employee will read the pertinent extracts of the Espionage Act of 1917, as amended and the CIG Security Regulations Manual. The Secrecy Agreement will then be read and executed under oath by the employee.

(2) He will be fingerprinted.

(3) He will be photographed.

Upon completion of the foregoing, the employee will be given an appointment slip instructing him to attend a security indoctrination class, which will be held within ten (10) days of his entrance-on-duty date. The employee will be requested to study carefully, and thoroughly familiarize himself with the instructions contained in the CIG Security Regulations Manual prior to attending the class.

b. *Indoctrination Class*

The Security Indoctrination class is conducted under the auspices of the Executive for Inspection and Security, and consists of:

(1) Presentation of a security film entitled "Security of Information";

(2) A one-hour security lecture and discussion of CIG Security Regulations;

(3) A short written examination on the subject of the CIG Security Regulations.

RESTRICTED

RESTRICTED

4

7. CHANGE OF STATUS

Whenever any changes occur in the personal status of an employee, such as change of address, marriage, etc., subsequent to his entry on duty, he will execute two copies of the Personal Status Report (CIG Form 38-17), with the changes underscored in red. The original copy will be sent to the Chief, Personnel Branch, and the duplicate to the Chief, Investigation Branch, Executive for Inspection and Security.

8. TERMINATION OF EMPLOYMENT OR LEAVE OF ABSENCE

Upon termination of duties with the Central Intelligence Group, all personnel will be given an exit interview designed to impress upon them their obligation with regard to maintaining the security of all matters pertaining to Central Intelligence Group activities, as well as the provisions of the applicable laws and statutes.

a. *Exit Interview*

Upon termination of employment, or upon commencing an extended leave of absence of sixty (60) days or more duration, employees must report to the Investigation Branch, Executive for Inspection and Security, for an interview by a Security representative. During the interview the employee will be advised of what he should or should not disclose concerning his duties, or concerning the work of the organization. The employee will also be questioned as to any security violations which might have come to his attention, and will be asked if he has any complaints or suggestions to make with regard to security. The employee will also surrender his CIG pass at this time.

b. *Leave of Absence*

Whenever an employee leaves Washington on vacation or official business in which the identification badge is not required, he is urged to turn his badge in to the Physical Security Branch for safekeeping during the period of absence.

III SECURITY OF BUILDINGS AND INSTALLATIONS

9. ADMITTANCE OF CIG EMPLOYEES AND OTHER GOVERNMENT PERSONNEL

All such persons entering, remaining in, or leaving CIG buildings during regular work hours will be required to display authorized identification credentials, as set forth below:

a. *Persons regularly employed by, or permanently assigned to CIG* will be furnished with numbered, rectangular photographic badges, as follows:

(1) *Green Bordered Badge* admitting bearer to all CIG buildings.

(2) *Yellow Bordered Badge* admitting bearer to all CIG buildings with the exception of Administration and Que Buildings. A holder of a yellow bordered badge may enter either of these two buildings without a visitor pass, by having the Receptionist confirm his appointment with the CIG staff member whom he wishes to see. The Receptionist will thereupon instruct the Guard to admit the employee, who, upon leaving the building, will merely be required to display his identification badge.

(3) *CIG Couriers and Messengers* will be issued Green Bordered Badges with the word "COURIER" stamped on the margin of the photograph in the badge. They will thus have access to all CIG buildings.

RESTRICTED

RESTRICTED

5

(4) Restricted Area—Signal Center, Communications Division, South Building

The guard stationed at that post will admit the holder of either a green or yellow bordered badge with a green band across the upper left hand corner. All other persons will be denied admittance to that area except on special permission of the Chief, Signal Center, or his superior.

b. *Employees of Certain Other Government Agencies temporarily assigned to CIG or those who, in the discharge of their official duties, are required to have frequent access to CIG offices, will be furnished, subject to the approval of the Executive for Inspection and Security, with numbered limited photographic passes, rectangular in shape, bearing issuance dates, names of persons to whom issued and signature of the Executive for Inspection and Security, as follows:*

(1) *Red Bordered Limited Badge* admitting bearer to those CIG buildings or areas specifically described thereon during the period for which it is issued, unless previously revoked.

c. *Lost Identification Badges.* In order to prevent possible compromise of security, it is important that holders of CIG identification badges exercise every precaution to prevent their loss or misuse. Lost badges must be reported at once to the Physical Security Branch, by the persons to whom issued, together with a written explanation of the circumstances of loss and efforts made to recover the missing badges. If a person should lose his badge while out of town, he should wire that fact to the Physical Security Branch.

d. *Inter-Agency Office Personnel, Contact Branch, O. O., assigned to the field, are authorized to take their yellow bordered badges, issued by the Physical Security Branch, with them when such badges are required in connection with their official duties. All other Inter-agency Office field personnel will deposit their badges for safe-keeping with the Physical Security Branch or with the Executive Officer, Contact Branch.*

e. *Issuance of Badges or Special Credentials.* Identification badges or special credentials will not be made or issued by any CIG office or organizational unit with the exception of the Physical Security Branch, Executive for Inspection and Security, or the Director, Central Intelligence, who, at his discretion, may issue certain credentials from time to time, which will be covered by special memorandum.

f. *Badge Limitations.* The bearers of CIG badges described in paragraphs "a" and "b" above, will have access to CIG buildings as indicated, but the possession of a badge does not imply full access to any and all parts of a building. All such persons entering CIG buildings will be subject to such internal security measures as Assistant Directors and Staff Chiefs may prescribe for the areas for which they are directly responsible.

g. *Public Buildings Administration maintenance employees* will be admitted upon displaying proper PBA identification badges issued by that agency. Special workmen will be admitted only by prior arrangement with the Executive for Inspection and Security. All such maintenance employees and special workmen admitted to CIG buildings during regular working hours will be required to sign the guard register upon entering and leaving the buildings.

(1) Except in an emergency, the only maintenance workers to be permitted to enter CIG buildings during nonwork hours shall be the members of the char

RESTRICTED

RESTRICTED

CENTRAL INTELLIGENCE AGENCY
Washington, D. C.

25X1A NOTICE

31 August 1950

SUBJECT: Admittance and Escorting of Visitors to CIA Buildings.

1. ADMITTANCE OF VISITORS. Casual or social visitors will not be permitted to enter CIA buildings, and staff members will not request exceptions to this rule. Visitors, as hereinafter referred to, shall be construed to mean persons on official business.

a. VISITS DURING REGULAR WORKING HOURS. All visitors shall be directed to the receptionist and thereafter admitted under escort to the building upon presentation of duly executed visitor passes. A visitor pass will not be issued by the receptionist unless authorized by the CIA staff member concerned with the interview. Upon completion of the visit, the interviewer will sign his name on the pass in ink and indicate the time of the visitor's departure.

b. VISITS DURING OFF DUTY HOURS. A person desiring to visit a CIA office during nonworking hours, including Saturdays, Sundays and holidays, will be required to execute a special visitor admittance form furnished by the guard after the latter has confirmed the appointment with the CIA staff member. The CIA staff member will sign the form, assuming responsibility for the visitor, and will escort the visitor from the guard desk. Upon completion of the interview, the staff member will escort the visitor from the building, at which time the visitor pass will be surrendered to the guard. The visitor, upon entering and leaving the building, also will sign the guard register.

c. ESCORTS.

(1) Each visitor to CIA buildings and areas will be escorted by the CIA interviewer, or a member of his staff, from the reception desk to his office. Upon completion of the interview the visitor will be escorted back to the reception desk. In addition, if it is necessary for a visitor to call upon two or more interviewers located in different offices within a CIA building or area, the first interviewer will escort the visitor to the second, etc., and the last interviewer will escort the visitor to the reception desk. Each interviewer will sign his name to the visitor pass and indicate the time of the visitor's departure.

RESTRICTED

RESTRICTED

(2) The Chief, Inspection and Security Staff, may waive the mandatory visitor escorting requirement in a particular building, when such action is warranted by unusual operating conditions which may exist therein.

d. SURRENDER OF PASS. The visitor pass shall be surrendered to the receptionist as the visitor leaves the building, or to the building guard if the receptionist has left for the day. The guard will turn over all collected visitor passes to the receptionist on the following morning.

2. The procedure set forth above supersedes paragraphs 10 a, b, c and d of existing Security Regulations dated 15 August 1947. These policies and procedures will be incorporated into the new Manual of Security Regulations when published.

FOR THE DIRECTOR OF CENTRAL INTELLIGENCE:

25X1A9a



Acting Executive

DISTRIBUTION: NO. 3

RESTRICTED

RESTRICTED

6

force and PBA engineers. No exceptions will be made without the approval of the Executive for Inspection and Security. All such persons will sign a special log at the guard desk upon entering and leaving the building.

(2) Staff members of CIG are warned to exercise caution with respect to conversation and exposed classified material when carpenters, electricians, telephone company employees, char people or other maintenance workers are present in their offices. Rooms must not be left unoccupied at such times unless classified material has been securely locked in suitable containers. Any attempt by such persons to overhear conversations or to read classified material should be reported at once to the Executive for Inspection and Security.

h. *Forgotten Identification Credentials.* Employees and holders of limited passes who forget their identification credentials will apply to the Receptionist for visitor passes in order to gain admittance to their offices. Before issuing such a pass the Receptionist will request that the applicant be identified by his superior or other responsible CIG staff member. The pass will be conspicuously marked "FORGOTTEN BADGE".

i. *Admittance to Buildings after Hours.* Employees and holders of limited passes who enter CIG buildings after 7:00 P. M. on Mondays through Fridays, or at any time on Saturdays, Sundays and holidays, will sign the Guard register upon entering and leaving buildings, in addition to displaying their identification credentials.

10. ADMITTANCE OF VISITORS

Casual or social visitors will not be permitted to enter CIG buildings, and staff members will not request exceptions to this rule. Visitors, as hereinafter referred to, shall be construed to mean persons on official business.

a. *Visitor Pass*

All visitors shall be directed to the Receptionist and thereafter admitted to the building upon presentation of duly executed visitor passes. A visitor pass, Form No. 38-4, will not be issued by the Receptionist unless authorized by the CIG staff member concerned with the interview. Upon completion of the visit, the interviewer will sign his name on the pass in ink and indicate the time of the visitor's departure under the heading "time out", in the space provided for that purpose in section 2 of the pass.

b. *Escorts*

As a general rule it shall not be necessary to provide escorts for visitors to and from offices of CIG. However, in certain circumstances as indicated below, escorting, for security or courtesy reasons, should be practiced.

If an appointment is made by the interviewer for a visitor with whom he is not acquainted, the interviewer, if he deems it advisable, may request the Receptionist to escort the visitor to his office. Upon completion of the interview, the CIG staff member may assign an office employee to escort the visitor from the building.

If, while arranging an interview, the Receptionist has reasonable doubt concerning a visitor, she may accompany him to the office of the interviewer. In such circumstances the interviewer will determine the advisability of assigning an office employee to escort the visitor from the building at the conclusion of the visit.

When an appointment has been made by the Receptionist and the visitor fails to make an appearance in the interviewer's office after the passage of a reasonable time, the latter will take such steps as may be necessary to determine the reasons for delay.

Suspended
dated 3/1/87
CIA

25X1A

RESTRICTED

RESTRICTED

7

When an unescorted visitor presents himself at the Reception desk in the process of leaving the building, and the Receptionist observes an unreasonable lapse of time since the visitor left the interviewer's office as indicated by the latter on the visitor pass under the heading of "time out", the Receptionist may make discreet inquiries of the visitor to determine the cause of delay. In such instances suspicious circumstances should be reported immediately by the Receptionist to the office of the Chief, Physical Security Branch, Executive for Inspection and Security, and to the interviewer.

As an act of courtesy, Receptionists should conduct prominent visitors to the offices of the interviewers.

Additional instructions regarding visitor control or other matters, to meet special conditions, may be issued to the Receptionists by the Executive for Inspection and Security, as circumstances warrant.

c. *Surrender of Pass*

The visitor pass shall be surrendered to the Receptionist as the visitor leaves the building, or to the building Guard if the Receptionist has left for the day. The Guard shall turn all collected Visitor Passes over to the Receptionist on the following morning.

d. *Visits During Off Duty Hours*

A person desiring to visit CIG offices during nonworking hours, including Saturdays, Sundays, and holidays, will be required to execute a special visitor admittance form furnished by the Guard after the latter has confirmed the appointment with the CIG staff member. The CIG staff member will sign the form, assuming responsibility for the visitor, and will escort the visitor from the Guard desk. Upon completion of the interview, the staff member will escort the visitor from the building, at which time the visitor pass will be surrendered to the Guard. The visitor, upon entering and leaving the building, will sign the Guard Register.

e. *Visitor Entrances*

Visitor entrances shall be confined to one for each building, with the exception of Que Building, in which there shall be two entrances for visitor use.

11. RECEPTIONIST STAFF

The Receptionist staff of CIG will be responsible for the courteous reception of visitors; discreet determination of the nature of the visits; arrangement of interviews; issuing visitor passes upon confirmation of appointments with the appropriate CIG staff members; issuing visitor passes to employees who have forgotten their identification credentials; providing escorts for visitors to and from the interviewers' offices when necessary; maintaining visitor logs in which are recorded visitors' names and addresses, names and room numbers of persons visited, and the general purposes of the visits; preparing reports related to the Receptionist operation; and will perform such other functions as may specifically be directed by the Executive for Inspection and Security.

12. GUARDS

a. Building Guards furnished by the Public Buildings Administration will admit into CIG buildings only those persons with proper identification credentials authorized for the respective buildings, and visitors to whom visitor passes have been issued.

*Suspended
Date 2/21
W/Curg 50*

25X1A

RESTRICTED

RESTRICTED

8

b. The Guards will patrol the offices after hours for the purpose of checking safes and windows, inspecting tops of desks and other equipment for exposed classified material, and maintain after-hour Guard Registers of visitors and employees who enter CIG buildings after hours or on Saturdays, Sundays and holidays. Security violations detected by the Guards during their patrols will be reported to the Physical Security Branch.

c. The Guards perform these functions under the orders and instructions of the Executive for Inspection and Security, and all members of CIG are expected to cooperate with the Guards in the performance of their duties.

13. KEYS TO OFFICES

Keys to offices will be kept at the Guard desks by the building Guards. Normally, offices will not be locked after regular duty hours. Staff Chiefs may cause to be locked any rooms they deem necessary for security reasons, upon prior arrangement with the Executive for Inspection and Security. Such rooms will be considered "RESTRICTED AREAS" and only specifically authorized persons will be admitted thereto by the guards. Persons not regularly assigned to "RESTRICTED AREAS" will not be permitted to enter such areas during regular work hours unless permission is granted by the staff chief of the area concerned.

IV SECURITY OF CLASSIFIED DOCUMENTS

14. DEFINITIONS OF CLASSIFICATIONS

a. *TOP SECRET*: Only that material or information, the unauthorized disclosure of which might cause *exceptionally grave damage to the Nation*, will be classified TOP SECRET. As a general rule, TOP SECRET matter in time of peace will be limited to that which, if disclosed without authorization, would reasonably be expected to lead directly to a definite break in diplomatic relations, or to a war, or have other exceptionally grave consequences.

Examples: Information or material regarding, or details of discussions or negotiations with, foreign governments on matters of great delicacy.

Information or intelligence material containing indications of sources of intelligence which the United States must protect.

Information or material concerning the existence or details of new devices or methods of warfare of extreme importance to national security.

b. *SECRET*: Information or material, the unauthorized disclosure of which might endanger national security, seriously jeopardize the international relations of the United States, or endanger the effectiveness of a program or policy of great importance to this Government, will be classified SECRET.

Examples: Information or material regarding, or details of discussions or conferences with high officials of foreign governments on important questions, the premature disclosure of which would seriously affect the foreign relations of the United States.

Reports or acts dangerously unfriendly to the United States, or important trends in foreign affairs greatly endangering national security.

Certain highly important intelligence reports, including reports on subversive activities.

RESTRICTED

RESTRICTED

9

Vital information on important defenses.

High-grade cryptographic devices and related material.

c. **CONFIDENTIAL**: Information or material, the unauthorized disclosure of which would not endanger national security, but which might prejudice the national interest or the work of any U. S. Government agency by interfering with the development or carrying out of important policy, or by hampering negotiations in progress; might cause serious administrative difficulties; or might result in unwarranted embarrassment of individuals, will be classified **CONFIDENTIAL**.

Examples: Important intelligence reports.

Reports concerning sabotage or subversive elements, or names of individuals involved.

Investigations, documents and communications of a personal and disciplinary nature, the knowledge of which must be safeguarded for administrative reasons.

d. **RESTRICTED**: Information or material which does not fall within higher categories, but which should not be communicated outside the Government of the United States without adequate clearance, will be classified **RESTRICTED**.

Examples: Matters related to internal organizational policy of a secondary character.

Routine internal reports.

Information of a nonconfidential nature, the use of which should be confined to official government activities and should not be publicly disseminated.

15. REGISTERED DOCUMENTS

a. *Definition and Identification*

A registered document is a **TOP SECRET**, **SECRET**, **CONFIDENTIAL** or **RESTRICTED** document, or a **RESTRICTED** cryptographic device, carrying a register number, a short title, and instructions to account for it periodically. A registered document is not to be confused with a classified document to which, for administrative reasons, a number or short title is assigned for bookkeeping or reference purposes only.

b. *Authority*

Documents will be registered only if it is essential for the issuing authority to control distribution and maintain a record of the custody of all copies. Officials of the CIG who originate or issue classified documents will request authorization to register only such documents as they deem necessary in the interest of national security. Each registered document issued after 1 January 1946 will be conspicuously marked "Registered Document" on the front cover. Documents will not be registered except on the authority of the Executive for Inspection and Security.

c. *Office of Record*

The office of record is the office to which reports of possession, transfer and destruction of registered documents are sent. The Central Records Division, Services Branch, Executive for Administration and Management, will be the office of record for registered documents originating within CIG.

16. AUTHORITY TO DETERMINE CLASSIFICATION

Documents and correspondence will be classified according to the provisions of paragraph 14, Section IV. The responsibility for insuring that documents produced

RESTRICTED

RESTRICTED

10

by CIG are properly classified rests with Assistant Directors or staff personnel occupying comparable positions, who will establish adequate procedures within their offices or staffs to provide for review of classifications given documents by their subordinate officials, in order to insure that correct and uniform classification techniques are applied. Overclassification must be avoided, for such practice will tend to weaken the entire security classification structure.

17. MARKING OF MATERIAL

Classified books, pamphlets or other multiple page documents, the pages of which are permanently and securely fastened together, will be plainly and conspicuously marked or stamped (not typed) "TOP SECRET", "SECRET", "CONFIDENTIAL" or "RESTRICTED" on the cover, title page, first page, back page, and outside of back cover. Classified matter not permanently and securely fastened together shall have the security classification stamped or marked (not typed) on the top and bottom of each page. All copies or reproductions shall be appropriately marked or stamped to correspond with the original thereof. Abstracts of documents will be marked in accordance with the provisions of paragraph 25, Section IV.

18. SAFEKEEPING OF DOCUMENTS

a. *Storage of Classified Documents* (including secretarial notes, carbons and stencils).

(1) *TOP SECRET documents* will be stored in safes or fire resistant safe-type file cabinets with not less than 3-way built-in combination locks.

(2) *SECRET and CONFIDENTIAL documents not Registered* may be stored in ordinary steel lock file cabinets equipped with vertical steel bars with combination type padlocks, *if combination safes or safe-type file cabinets are not available*. Every effort should be made to store SECRET documents in combination safes.

(3) *RESTRICTED documents not Registered* should be stored in ordinary steel lock file cabinets, but they may be kept in desks, cabinets or other storage places where they will be out of view.

(4) *REGISTERED documents*, irrespective of classification, will be stored in combination safes or safe-type file cabinets.

(5) **ARMED GUARD.** In certain unusual circumstances, or if, for operational reasons, it is not possible to apply the foregoing storage requirements, arrangements may be made, subject to the approval of the Executive for Inspection and Security, to safeguard the documents under armed guard, when not in use.

b. *General*

The safekeeping of classified documents is of prime importance. The foregoing storage requirements, prescribed for the various security classifications, must be strictly adhered to. Documents classified above RESTRICTED will not be kept in locked desks or other substitutes, nor will they be left unprotected at any time. Classified material will not be taken home. All work thereon must be performed in the office where it can be fully protected. Precautions should be taken to prevent unauthorized persons from seeing classified documents while work is being performed on them.

19. SAFES

a. Each combination safe and safe-type file cabinet will have a sticker applied inside the container on which will be recorded the name of the person responsible for

RESTRICTED

1713
RKC

RESTRICTED

CENTRAL INTELLIGENCE AGENCY
Washington, D. C.

25X1A

NOTICE

20 June 1950

SUBJECT: Rescission of Paragraph 21 of the Security Regulations,
dated August 1947.

1. Paragraph 21, pages 11 and 12, of the Security Regulations
dated August 1947 is hereby rescinded, and the following instructions
substituted therefor:

21. DESTRUCTION OF CLASSIFIED DOCUMENTS

a. The destruction of classified documents must be
accomplished in accordance with existing law and regulations.
The law provides that government records may not be destroyed
without the approval of the Archivist of the United States
and the Congress of the United States. Custodians of docu-
ments will survey periodically all such material in their
possession and, if deemed of no further use, will request
their Area Records Officer to review the documents and give
directions for appropriate disposition as provided in the
CIA regulations on Records Management.

b. TOP SECRET DOCUMENTS, NOT REGISTERED, will be
destroyed by burning by the custodian thereof or his
designee at the CIA incinerator, in the presence of a
witnessing CIA member. The custodian or his designee,
and the witness, will remain at the incinerator until
all the documents have been burned completely. The
appropriate Area, Alternate or Assistant Top Secret Control
Officer must be notified of the destruction in order that
the proper entries may be made on the Top Secret Log.
When a Top Secret document is destroyed, the disposal
certificate portion of the Signature Record and Cover
Sheet, attached to the document, will be executed. The
cover sheet will then be forwarded to the CIA Top Secret
Control Officer, through the appropriate Area Top Secret
Control Officer. Paragraphs 21. a., h. and i. of this
section also must be complied with.

c. SECRET, CONFIDENTIAL AND RESTRICTED DOCUMENTS,
NOT REGISTERED, may be destroyed by burning by the cus-
todian thereof or his designee at the CIA incinerator, or
such documents may be shredded or torn into small pieces
and placed in the classified waste receptacle, for subsequent

RESTRICTED

burning by the Physical Security Branch. Under no circumstances will whole documents be placed in the classified waste receptacles. A witness to the destruction is not required. Paragraphs 21. a., h. and i. of this section also must be complied with.

d. REGISTERED DOCUMENTS, will be destroyed by burning, by the Area Custodian of Registered Documents, or his designee, at the CIA incinerator, in the presence of a witnessing CIA member. Such persons will remain at the incinerator until all the documents have been burned completely. Before a Registered document may be destroyed, authorization must be obtained by the Area Custodian (with the exception of the Communications Division) from the CIA Custodian of Registered Documents. With respect to Registered Top Secret Documents, all requirements pertaining to the destruction of Unregistered Top Secret Documents, as set forth in subparagraph b., above, must be observed also. In addition, paragraphs 21. a., h. and i. of this section, also must be complied with.

e. CLASSIFIED DOCUMENT RECEIPTS. CIA Document Receipts which reflect the issue and receipt of specific classified documents may be destroyed, in accordance with the provisions of subparagraph c., above, as follows:

(1) Top Secret and Registered Document Receipts, after five years.

(2) Unregistered Secret, Confidential and Restricted Document Receipts, after two years.

f. CIA COURIER RECEIPTS which reflect the receipt and delivery of packages containing classified documents may be destroyed after one year in accordance with the provisions of subparagraph c., above.

g. BURN TEAMS. Chiefs of Offices, Staffs and Divisions may, if they wish, organize "burn teams" for the purpose of destroying documents in accordance with the provisions of subparagraphs a-b-c-e-f, above, provided unauthorized access is not permitted thereby. Central collecting points for documents to be destroyed by the "burn teams" may be established in offices or areas.

h. PERSONS ASSIGNED TO BURN CLASSIFIED DOCUMENTS AND THOSE SELECTED AS WITNESSES.

Office Chiefs will assure themselves that persons assigned to burning and witnessing duties, in accordance with the provisions of this instruction, are authorized to have access to the material to be destroyed, and that they are dependable and thoroughly familiar with the security requirements involved. Such persons need not be of any minimum grade or rank.

RESTRICTED

1. CERTIFICATES OF DESTRUCTION

(1) For All Unregistered Top Secret Documents, a Certificate of Destruction will be executed, in duplicate, and signed by the custodian or his designee and the witness. The Certificate will include, in addition to the signatures, the date, name of organizational unit, and an itemized list of the documents and their classifications. Document Receipts for Top Secret documents, when destroyed after the required retention period, will not be listed on the Certificate of Destruction. The original copy of the Certificate will be sent to the Records and Files Section, Central Records Branch, OCD.

(2) For Unregistered Secret, Confidential and Restricted Documents, which must be accounted for to the originating office or agency by specific instructions, a Certificate of Destruction will be executed, in duplicate, and signed by the custodian or his designee. A witness to the destruction will not be required. The Certificate will include, in addition to the signature of the custodian or his designee, the date, name of organizational unit, and an itemized list of the documents and their classifications. Document Receipts for such documents, when destroyed after the required retention period, will not be listed on the Certificate of Destruction. The original copy of the Certificate will be sent to the Records and Files Section, Central Records Branch, OCD.

(3) For Unregistered Secret, Confidential and Restricted Documents, which carry no specific accountability requirements to the originating office or agency, a Certificate of Destruction for records management purposes, will be prepared in duplicate and signed by the custodian or his designee. A witness to the destruction will not be required. The Certificate will include, in addition to the signature of the custodian or his designee, the date, name of organizational unit, identification and security classifications of the file series destroyed, and the volume of the documents in approximate linear inches or feet. The volume of the material listed on the Certificate of Destruction will include the documents destroyed by burning and those disposed of in the classified waste. The original copy of the Certificate will be sent to the Records and Files Section, Central Records Branch, OCD.

(4) Registered Documents. Certificates of Destruction for all Registered Documents of all classifications, will be prepared in the same manner as that prescribed for Unregistered Top Secret Documents, with the exception that the original copy of the Certificate will be forwarded to the CIA Custodian of Registered Documents.

RESTRICTED

2. The above instructions will be incorporated in the revision of the Security Regulations at an early date.

FOR THE DIRECTOR OF CENTRAL INTELLIGENCE:



Acting Executive

25X1A9a

DISTRIBUTION: A.

RESTRICTED

RESTRICTED

11

the safe, his home address and telephone number, the names, home addresses and telephone numbers of all other persons in possession of the combination, listed in the order of principal use, and the date when the combination was last changed. The sticker will be placed on the side and near the front panel of each drawer of the conventional safe-type file cabinet, and on the inside of the door of the Mosler safes. Scotch tape should be placed over the sticker to properly secure it. The person responsible for a safe is also accountable for its proper working condition. He should arrange for the immediate repair of any defective safekeeping equipment in his custody. Combinations of safes and safe-type file cabinets will be known to only those persons who are required to have access to them in the performance of their official duties. Combinations of all safekeeping equipment will be changed at least once every six months. If a person having knowledge of the combination of a safe should leave the organizational unit or CIG, the combination of the safe involved will be changed immediately. It is the responsibility of custodians to have the combinations changed in accordance with these requirements: A representative of the Physical Security Branch will make the change upon request by the custodian. The Physical Security Branch alone will change the combinations of CIG safes, with the exception of those located in the Office of Special Operations.

b. A number will be assigned to each safe by the Physical Security Branch. The person responsible for a safe or safe-type file cabinet will turn the combination of the safe over to the Physical Security Branch, double-wrapped in sealed envelopes (inner envelope marked "TOP SECRET"), signing his name on the flap of the outer envelope. The combination of a safe may be obtained from the Physical Security Branch by the person whose signature appears on the flap of the envelope or by his staff chief, upon proven necessity and receipt therefor. A safe combination will never be divulged over the telephone, except in an extremely grave emergency, following which the combination will be promptly changed.

20. DISPOSITION OF CLASSIFIED WASTE

Preliminary drafts, copies, carbons, stencils, stenographic notes, work sheets, and the like, pertaining to classified matter will be torn or shredded and placed in envelopes marked "SECRET". *Waste baskets will be used for unclassified waste only.* The envelopes containing the classified waste may be disposed of daily by placing the contents in sacks maintained for that purpose at the guard desks at the main entrances to CIG buildings or areas. The sacks are picked up and the waste burned daily. Classified waste, until disposed of in the sacks, must be safeguarded in the same manner as SECRET documents.

21. DESTRUCTION OF CLASSIFIED DOCUMENTS

Destruction of classified documents must be accomplished in accordance with existing law and regulations. The law provides that government records may not be destroyed without the approval of the Archivist of the United States or the Congress of the United States. Custodians will survey periodically all such documents in their possession and, if deemed of no further use, will transmit same to the Central Records Division for appropriate disposition, with the following qualifications: drafts, unless used for obtaining necessary concurrences, extra copies, preserved solely for convenience or reference and not parts of integrated files, publications distributed by the Central Records Division, routine buckslips and courier receipts which are no longer current,

See
re-
vision
of
20 June
50

RESTRICTED

RESTRICTED

12

may and should be destroyed by the custodian by burning in accordance with the provisions of paragraphs "a" and "b" below. Due to the restrictions imposed by the Congress on the destruction of Government records, the custodian should consult the Central Records Division in any case where there is doubt concerning the propriety of the destruction of a particular paper or document.

a. *TOP SECRET, SECRET, CONFIDENTIAL and REGISTERED RESTRICTED documents* must be burned in the presence of the custodian thereof, and witnessed by a disinterested official. The witness will be an officer of the Army or Navy, or a civilian in a grade of P-3, CAF-9, or higher. A certificate of destruction will be executed in duplicate, and signed by both the custodian and the witnessing official. The certificate will include, in addition to the signatures, the date, name of organizational unit, certification, and a list of the documents and their classifications. The original copy of the certificate will be forwarded to the Central Records Division for filing and the duplicate copy will be retained by the custodian for his records.

(1) Classified documents may be burned at any time during the work day at the incinerator located in the North Building, where an attendant is on duty to assist in the work.

b. *RESTRICTED documents not Registered* may be disposed of by burning, or by shredding and placing in envelopes marked "SECRET" as provided for in the procedure regarding the "Disposition of Classified Waste," paragraph 20, Section IV. Waste baskets will not be used for disposing of RESTRICTED documents. The destruction of RESTRICTED material need not be witnessed, nor is it necessary to maintain a record of the documents destroyed.

22. RESTRICTIONS ON DISSEMINATION OF CLASSIFIED INFORMATION

Any person on duty with CIG who, with deliberate intent or through gross negligence, causes classified information affecting the national security to be conveyed to unauthorized persons is subject to the penalties provided for by the Espionage Act. Public or private discussion of classified data with, or in the presence or hearing of, any person not authorized to have knowledge thereof is strictly forbidden. CIG members will refrain from giving unauthorized persons any information about their work. The following description of the Central Intelligence Group is public knowledge, and CIG members are at liberty to quote therefrom if they should be asked about the organization:

The Central Intelligence Group is a recently created inter-departmental organization in which the State, War, Navy and sometimes other departments participate. It coordinates all activities of the government involved in obtaining and analyzing information about foreign countries which this country needs for its national security. It also furnishes inter-departmental analyses of this type of information for use of government officials.

No amplification of the foregoing statement to unauthorized persons will be permitted.

23. LOSS OR COMPROMISE OF CLASSIFIED DOCUMENTS

In case of loss or compromise of classified documents or information, immediate notification thereof will be made to the Executive for Inspection and Security.

24. CLASSIFICATION ADJUSTMENTS

a. Staff Chiefs or their designees should periodically review classified documents in the custody of their respective organizational units, with a view to cancelling

See
revision
of
20 June
50

RESTRICTED

RESTRICTED

13

or downgrading the classifications of those documents, the security significance of which has declined or ceased to exist. The person making the original classification, his successor or superior, may cancel or modify the classification of a document, by reason of changed conditions or over-classification, by stamping or writing over the classification at the top of the cover or first page "Classification Cancelled or Changed to by Authority of," adding the date and name of the person authorizing the change.

b. In the course of review, consideration should also be given to the upgrading of documents which occasionally will be found to have been assigned inadequate classifications.

c. In cases wherein appropriate authority to effect changes in classification is not readily determinable or available, questions of policy and procedure may be referred to the Control Division, Requirements Branch, OCD, or if then not resolved, to the Security Control Staff, Executive for Inspection and Security.

d. When the classification of a document is altered, steps should be taken, in so far as practicable, to change the classification of all copies thereof correspondingly. Offices of origin, when changing the classifications of documents, should so inform all persons to whom such documents had been distributed, if the recipients are readily determinable.

25. DUPLICATING OR ABSTRACTING OF CLASSIFIED DOCUMENTS

a. Duplication of classified material by the originating office shall be limited to the number of copies necessary for efficient operation.

b. Classified documents will not be duplicated without authorization of the office of origin.

c. Abstracts of classified documents may be made with the approval of the office of origin. The abstract, however, will not necessarily bear the same classification as the document from which it was taken, but will be classified on its own merits, with the concurrence of the office of origin.

d. The originating office will maintain a record of the distribution of classified material, including the names of the recipients and the number of copies assigned to each.

26. TOP SECRET CONTROL PROCEDURE

The TOP SECRET Control Procedure prescribed herein is established to provide a secure system for the handling of TOP SECRET material and to insure that unauthorized persons may in no instance have access to such material. To achieve these aims is a primary responsibility of all CIG personnel.

a. *Control Officers*

The TOP SECRET Control Officer and Alternate TOP SECRET Control Officers will be persons of highest integrity and proven discretion, specifically authorized to transmit and receipt for TOP SECRET material to and from agencies *outside* of CIG. The TOP SECRET Control Officer will be appointed by the Director, CIG. Alternate TOP SECRET Control Officers will be nominated by assistant directors and chiefs of branches of the Executive Staff. Their names will be forwarded to the TOP SECRET Control Officer who will submit the approved names thereof to the Executive for Administration and Management for publication in Personnel Orders. The Chief, Central Records Division, Services Branch, Executive for Administration and

RESTRICTED

RESTRICTED

14

Management, all TOP SECRET couriers, and certain other appointed officers and civilians will be the authorized TOP SECRET Control Officer and Alternate TOP SECRET Control Officers for CIG. A list of the names of these officers will be maintained by the TOP SECRET Control Officer, who will notify the Executive for Inspection and Security as changes occur. The names of the TOP SECRET Control Officer and alternates for each government establishment in this vicinity are periodically announced in classified form, by the Joint Security Control, Joint Chiefs of Staff, to each Federal agency, organization or office in the Washington area. The Executive for Administration and Management will periodically forward to the Joint Security Control an up-to-date list of the CIG TOP SECRET Control Officer and his alternates.

b. *Assistant Control Officers*

Assistant TOP SECRET Control Officers will be officers and civilians who are considered by the appointing officials to be of the highest integrity and proven discretion, authorized to transmit, receive and receipt for TOP SECRET material *within* CIG. The number of Assistant TOP SECRET Control Officers is necessarily kept at a minimum consistent with security of TOP SECRET material and its efficient handling in the office concerned. Assistant TOP SECRET Control Officers will be appointed by Assistant Directors and Chiefs of Branches of the Executive Staff for their respective offices. A list of the names of such officers will be maintained by the Chief, Central Records Division, and it is the responsibility of the appointing officials to notify the Chief, Central Records Division, of all changes, additions or deletions of Assistant TOP SECRET Control Officers which take place within their respective jurisdictions. The Chief, Central Records Division, will, in turn, notify the Executive for Inspection and Security as changes occur.

c. *Responsibility of Control and Assistant Control Officers*

The TOP SECRET Control Officer, his Alternates and Assistant TOP SECRET Control Officers will be responsible for the security of TOP SECRET material in their custody. They will insure that such matter is received, transmitted, processed and safeguarded in accordance with the security provisions contained herein.

d. *Clearance for users of TOP SECRET material*

Chiefs of offices and staff branches will be held responsible for the designation of persons within their own offices, other than Alternate and Assistant TOP SECRET Control Officers, who they deem are operationally required to see TOP SECRET material, and they are further responsible that necessary controls are exercised to confine the number of such persons to the minimum.

e. *Security Check*

The Executive for Inspection and Security will conduct periodic and unannounced checks of offices of CIG to determine whether sound security measures are being practiced, and whether the Security Instructions pertaining to TOP SECRET material are being observed.

27. **PROCESSING OF INCOMING TOP SECRET MATERIAL**

All TOP SECRET material (except cables and documents pertaining solely to the Office of Special Operations) should be delivered initially to the Special Distribution Section, Central Records Division. If a CIG member receives a TOP SECRET document directly from an outside agency, he will notify the Central Records Division in order that the document may be properly recorded.

RESTRICTED

RESTRICTED

15

a. *Signature Record and Cover Sheet*

Each incoming TOP SECRET document will be recorded by the Special Distribution Section, Central Records Division, and will have a CIG Control Number assigned to it. A TOP SECRET Signature Record and Cover Sheet, Form No. 38-13, will be *stapled* to the document to serve as a permanent record within CIG. This form, green in color, will not be removed from the document until it is destroyed, downgraded, or dispatched to an organization outside of CIG. If the document is disposed of, the Special Distribution Section, Central Records Division will note the nature of the disposition on the Signature Record and Cover Sheet, remove the form and file it.

(1) The Signature Record and Cover Sheet, Form No. 38-13, for TOP SECRET documents will be attached by the preparing office when such material originates within CIG. Control numbers will be assigned to such documents by the Special Distribution Section, Central Records Division, only if they are dispatched to agencies outside of CIG.

(2) Each CIG member receiving TOP SECRET material will sign his name on the Signature Record and Cover Sheet, Form No. 38-13, and indicate the date and time of receipt. Upon releasing the document, he will initial the sheet, indicate the date and time of release, and obtain the signature of the recipient. The Cover Sheet will thus serve as a permanent record of those persons who had access to the material.

b. *TOP SECRET Log*

After recording and affixing a Control Number and the Signature Record and Cover Sheet, Form No. 38-13, to a TOP SECRET document, the Special Distribution Section, Central Records Division, will deliver it by TOP SECRET courier to the Assistant TOP SECRET Control Officer of the organizational unit concerned. The latter official will record the document in his TOP SECRET log and turn it over to the individual to whom it is addressed or to the authorized person, if not specifically addressed. The Assistant TOP SECRET Control Officer will obtain the signature of the recipient in his log. The same log procedure will be followed by all subsequent recipients of the document within CIG.

(1) If a TOP SECRET document is delivered from the jurisdiction of one Assistant TOP SECRET Control Officer to another within CIG, the Central Records Division will be notified so that the change of responsibility may be properly recorded.

c. *Deviations*

Deviations from the TOP SECRET Control Procedures set forth herein may be made only with the express permission of the TOP SECRET Control Officer.

28. TRANSMISSION OF CLASSIFIED DOCUMENTS OUTSIDE CIG

a. *TOP SECRET Documents* will be double wrapped, unless hand delivered by the TOP SECRET Control Officer or an Alternate TOP SECRET Control Officer, and document receipts will always be obtained. The recipient's signature in the sender's TOP SECRET Log Book is equivalent to a document receipt. Only TOP SECRET couriers or approved electrical means will be utilized for the transmission of TOP SECRET documents, unless hand delivered by the TOP SECRET Control Officer or an Alternate TOP SECRET Control Officer. When hand delivered by the TOP SECRET Control Officer or an Alternate, the Central Records Division, Services Branch, Executive for Administration and Management, will be notified of the change in custody. Under

RESTRICTED

RESTRICTED

16

no circumstances may TOP SECRET documents be transmitted by Registered Mail. A TOP SECRET Log Book will be maintained for the receipt and disposition of all TOP SECRET documents.

(For detailed instructions see Appendix "A" of this manual.)

b. *SECRET and CONFIDENTIAL Documents Not Registered* will be double wrapped, unless hand delivered by the custodians thereof. Document receipts will be obtained for SECRET documents, but not for CONFIDENTIAL documents unless the sender deems it necessary. The recipient's signature in the sender's SECRET and CONFIDENTIAL Log Book is equivalent to a document receipt. Only authorized couriers, approved electrical means or Registered Mail will be utilized for outside transmission of SECRET and CONFIDENTIAL documents, unless hand delivered by the custodian thereof. A SECRET and CONFIDENTIAL Log Book will be maintained for the receipt and disposition of all such documents.

(For detailed instructions see Appendix "A" of this manual.)

c. *RESTRICTED Documents Not Registered* may be delivered by messenger, any office assistant, or by regular mail. Such documents need not be double wrapped, nor is it necessary to obtain document or envelope receipts for them. From the stand-point of security, a log for RESTRICTED documents need not be maintained, but the custodian will be held responsible for such documents with respect to records accountability.

(For detailed instructions see Appendix "A" of this manual.)

d. *Registered Documents*

Registered TOP SECRET documents will be transmitted in the same manner as unregistered TOP SECRET documents. Registered SECRET, CONFIDENTIAL and RESTRICTED documents will be transmitted in accordance with the procedure prescribed for unregistered SECRET documents, with the exception that the Central Records Division will be notified of change in custody when the custodian hand-delivers the document to an outside agency. A log will be maintained for the receipt and disposition of all registered documents, irrespective of classification, with the exception of registered TOP SECRET documents, which will be recorded in the TOP SECRET Log.

e. *Maintenance of Logs*

TOP SECRET Logs will be maintained by alternate or assistant TOP SECRET Control Officers. *Secret and Confidential Logs* will be maintained by the custodians of the documents or by such other responsible persons specifically designated for that purpose by office chiefs.

29. TRANSMISSION OF CLASSIFIED DOCUMENTS WITHIN CIG

a. *TOP SECRET Documents* will be double wrapped, unless hand delivered by the custodian, TOP SECRET Control Officer, Alternate TOP SECRET Control Officer or Assistant TOP SECRET Control Officer. Document receipts will be obtained in all cases. The recipient's signature in the sender's TOP SECRET Log Book is equivalent to a document receipt. Only TOP SECRET couriers, the TOP SECRET Control Officer, Alternate TOP SECRET Control Officers, Assistant TOP SECRET Control Officers, or the custodian thereof may effect delivery of a TOP SECRET document *within* CIG. A TOP SECRET Log Book will be maintained for the receipt and disposition of all TOP SECRET documents.

RESTRICTED

RESTRICTED

17

(For detailed instructions see Appendix "A" of this manual.)

b. *SECRET and CONFIDENTIAL Documents Not Registered* will be enclosed in a single CHAIN ENVELOPE (no further cover required) and sealed by means of a CIG gummed label. Under no circumstances will scotch tape be used for sealing purposes on the CHAIN ENVELOPE. The CHAIN ENVELOPE will bear no marking to indicate the classification of its contents. Double wrapping may be substituted for the CHAIN ENVELOPE if, due to the nature of the document's contents, the sender deems additional precautions advisable. Envelope receipts will be obtained in all cases except when hand delivered by the custodian, in which event the CHAIN ENVELOPE need not be used. Document receipts will be obtained only when the sender deems it necessary. The recipient's signature in the sender's SECRET and CONFIDENTIAL Log Book is equivalent to a document receipt when such a receipt is required by the sender. Messengers, custodians or any office assistant may effect delivery of SECRET and CONFIDENTIAL documents within CIG buildings. Authorized couriers, custodians or any responsible office assistant may make deliveries of such documents between CIG buildings. A SECRET and CONFIDENTIAL Log Book will be maintained for the receipt and disposition of all such documents.

(For detailed instructions see Appendix "A" of this manual.)

c. *RESTRICTED Documents Not Registered* may be delivered by messenger or any office assistant. When the messenger service is utilized, the document will be enclosed in a single CHAIN ENVELOPE (no further cover required). The CHAIN ENVELOPE will bear no marking to indicate the classification of its contents. CHAIN ENVELOPES need not be used when deliveries of RESTRICTED documents are made by office assistants. Document or envelope receipts need not be required in any case. From the standpoint of security, a log for RESTRICTED documents need not be maintained, but the custodian will be held responsible for such documents with respect to records accountability.

(For detailed instructions see Appendix "A" of this manual.)

d. *Registered Documents*

Registered TOP SECRET documents will be transmitted in the same manner as unregistered TOP SECRET documents. Registered SECRET, CONFIDENTIAL and RESTRICTED documents will be transmitted in accordance with the procedures prescribed for unregistered SECRET documents. A log will be maintained for the receipt and disposition of all registered documents, irrespective of classification, except TOP SECRET, which will be recorded in the TOP SECRET Log.

e. *Maintenance of Logs*

See paragraph 28-e, Section IV.

V GENERAL SECURITY PRACTICES

30. SECURITY IN OFFICE ROUTINE

Since effective security is largely a matter of habit, each office must be run on a set routine designed to insure complete security. Daily operations should be performed in such a manner that security at no time will be compromised.

a. *Telephone*

(1) The presumption must be that every conversation by telephone or inter-office communication system will be overheard by unauthorized persons. No wires

RESTRICTED

RESTRICTED

18

are protected, not even those carrying inter-office calls. Therefore, TOP SECRET, SECRET, or CONFIDENTIAL information must never be discussed over such facilities.

(2) When answering the telephone, an employee will give the name of the person whose office is called, e.g., "Mr. Smith or Mr. Smith's office." Switchboard operators will answer "Central Intelligence Group" to calls from outside CIG. When a person requests information over the telephone and there is any doubt regarding his identity or the necessity of his requiring the information, the employee will take his name and telephone number and offer to return the call. The employee will then discuss the request with his superior and decide upon a reply. Employees will not transmit information about CIG to unknown or unauthorized persons.

b. *Safes*

A large sign marked "OPEN" will be inserted in the handle of the top drawer of each safe-type file cabinet and on the handle of each Mosler type safe during the time such equipment is unlocked. This is intended as a visual warning to custodians or other office employees to lock safes at the end of the day or during unguarded periods within the regular work day.

c. *Unoccupied Rooms*

Employees will not leave rooms unoccupied at any time during the day if classified documents are exposed in the office. If it is necessary to leave a room unoccupied, all material classified above "RESTRICTED" first must be securely locked in the proper safekeeping equipment or temporarily placed in another employee's custody. During such periods, classified documents will not be placed in desks, or under trays or desk pads.

d. *Visitors*

No employee will permit classified papers to be exposed on his desk in such a fashion that they could be read by persons visiting his office who are not authorized to have such information. At such times classified material should be turned face down on the desk.

e. *Classified Waste*

Classified waste must be disposed of in accordance with the regulations governing the disposition of such matter. Waste baskets will not be utilized for that purpose.

f. *Defective Storage Equipment*

Employees will immediately report defective safekeeping equipment to their superiors who, in turn, will promptly request the Physical Security Branch to make the necessary repairs. In the meantime, classified material should be transferred from the faulty containers to properly functioning, appropriate safekeeping equipment.

g. *Securing Office at End of Day*

Each member of CIG will take the following steps to insure the security of his area before departing for the day:

(1) Clear desk of all material classified above RESTRICTED and lock it in appropriate safekeeping equipment.

(2) Invert "In" and "Out" trays, or turn them on their sides.

(3) Determine that classified waste has been properly disposed of or is locked in safe.

RESTRICTED

RESTRICTED

19

(4) Check safes, unless safe custodian is still present, to see that they are securely locked, rotating the dial knob at least three times in each direction. Custodians or users of safes will execute the Security Check Sheet, Form No. 38-7, attached to the top or side of each safe and safe-type file cabinet, indicating that the equipment has been properly locked.

(5) As a double check, the last person to leave the room will make certain that the above security measures have been taken, that the windows are locked and the lights extinguished.

31. SECURITY OUTSIDE OF OFFICE

a. *Discussion of CIG Activities*

Employees will not discuss their work or the activities of CIG outside of the office, except as may be required in the performance of their official duties.

b. *Credit Reference*

In using CIG as a credit reference, employees will refer inquiries to:

Mrs. [REDACTED]
Assistant Personnel Officer
Central Intelligence Group
2430 "E" Street, N. W.
Washington 25, D. C.

25X1A9a

With the above exception, employees will not furnish the names of their superiors, other CIG employees, or units of organization, for credit reference purposes.

c. *Traffic Accidents, Arrests, Court Proceedings*

If an employee should become involved in a traffic accident, court proceedings or other external affair in which CIG might become directly or indirectly involved, even though the matter be almost entirely personal, he should report the affair to his superior at the earliest opportunity in order that suitable security measures may be taken by the Executive for Inspection and Security.

d. *Group Social Activities*

In the interest of security, group social activities of CIG personnel, such as annual parties, picnics, dances, athletics, will not be advertised as CIG functions.

32. STAFF SECURITY CHECK

a. Each office chief will organize a group of Staff Duty Officers to conduct daily, final after-hour security checks of the area occupied by that staff. The Staff Duty Officers will be rotated, one serving each evening, and will be selected from among the officers and responsible civilian personnel of the office staff.

b. The Staff Duty Officer will begin his security check after the end of the regular work day when all or most of the employees have left. If an employee is working late, he will be informed by the Staff Duty Officer that he, the employee, will be responsible for the security of his own immediate room or area, and the Staff Duty Officer will so note on his Staff Duty Officer Check Sheet, Form No. 38-8, under "Remarks". During the course of his security check, the Staff Duty Officer will execute a Staff Duty Officer Check Sheet, Form No. 38-8, which will include the listing of any security violations. The Check Sheet will be forwarded to the Physical Security Branch immediately the following morning.

RESTRICTED

RESTRICTED

20

- c. The Staff Duty Officer will check to insure that:
 - (1) All safes and safe-type files are locked.
 - (2) No material classified above RESTRICTED has been left exposed on desks, on other office equipment, or on the walls.
 - (3) All classified waste has been properly secured.
 - (4) Classified material has not been discarded in waste baskets.
 - (5) All windows are locked.
 - (6) Lights are extinguished in unoccupied rooms, unless otherwise specified.

33. NIGHT DUTY OFFICERS—SECURITY ONLY

a. A staff of Night Duty Officers, attached to the Office of the Executive for Inspection and Security, will be assigned to security duties during all nonworking hours, Mondays through Fridays, and twenty-four (24) hours on Saturdays, Sundays and holidays.

b. Night Duty Officers will conduct nightly security checks of CIG buildings, usually one building or an area within a building each night. No set pattern or rotation system with respect to the buildings to be inspected will be followed. The building to be checked is determined daily by the Physical Security Branch.

c. In conducting their security checks, the Night Duty Officers will check the tops of desks and other equipment for exposed classified material, safes, windows, classified waste envelopes and will note conditions presenting security hazards. These Officers will also conduct spot checks of desk drawers to determine whether they contain classified material above RESTRICTED, in violation of safekeeping regulations.

d. The Night Duty Officers will respond to reports from the PBA Guards in connection with open safes and exposed classified material detected by the members of the guard force in the course of their night patrols; handle all other routine after-duty hour security problems and prepare reports of security violations, which are subsequently forwarded to the appropriate CIG officials by the Executive for Inspection and Security.

VI SECURITY OF FIELD INSTALLATIONS

34. CLEARANCE OF PERSONNEL

Unless specifically excepted in the name of the Director, all personnel of foreign installations of CIG must comply in every respect with the provisions of Section 102 of the Manual of Administrative Instructions and are subject to the same regulations, practices and procedures pertaining to personnel security matters as are hereinbefore set forth.

35. PHYSICAL SECURITY

In general, all physical security measures as previously outlined herein are also applicable to field installations. It is realized, however, that local conditions, the type of work being performed, and other considerations, may warrant change or deviation from some of the procedures and practices in effect within the Washington area. Additional orders, directives, regulations, and procedures will be formulated and issued at a later date on matters pertaining to Security of Field Installations.

August 15, 1947

RESTRICTED

RESTRICTED

APPENDIX "A"

(Abstracted from the Communications chapter of the Manual of Administrative Instructions)

I USE OF CIG INTER-OFFICE CHAIN ENVELOPE

1. GENERAL

a. *When Used*

Offices of CIG will use the official CIG inter-office chain envelope for the transmittal of documents below TOP SECRET in classification traveling within the CIG Messenger and Courier System to other offices of CIG. Under no circumstances will the envelope be used for the transmittal of TOP SECRET documents. Documents will not be transmitted outside CIG in the inter-office chain envelope.

b. *Stocking of Inter-Office Chain Envelope*

Each office Message Center as well as pick-up and delivery points within offices will, upon request to Central Records Division, Services Branch, be furnished with a supply of inter-office chain envelopes.

c. *Delivery of Mail*

All mail delivered by a Messenger or Regular Courier to an Office Message Center or a pick-up and delivery point within an office will be contained in CIG inter-office chain envelopes. Where mail is classified SECRET or CONFIDENTIAL, the responsible individual at a delivery point will remove attached Receipt Form 35-16 from the inter-office chain envelope, sign, and return signed receipt to the Messenger or Courier. Normally, chain envelopes containing Restricted or unclassified mail will bear no receipt.

2. DISPATCHING OF CIG DOCUMENTS IN INTER-OFFICE CHAIN ENVELOPES

a. *Additional Wrapping Not Necessary*

Offices of CIG will dispatch outgoing inter-office mail (and that intra-office mail which is destined for a segment of an office housed in a separate building) in CIG inter-office chain envelopes without additional wrapping. A separate inter-office chain envelope will be prepared for each office to which materials are being sent.

b. *Preparation of Face of Envelope*

It is essential that the columns appearing on the inter-office chain envelope be filled in completely, and that the office designation always be indicated. If it is the desire of the sender to dispatch the document to a specific individual, the individual's name may be noted in parentheses after the office designation, for example:

FROM: OCD TO: ORE (Attn: Mr. Blank)

In all instances room number, when known, and building will be indicated in the proper column. The CIG inter-office chain envelope will not be thrown away until all spaces have been used, or until the envelope is completely worn out. If an office accumulates a stock of envelopes which exceeds its needs, the surplus will be returned to the Messenger or Courier serving the office.

c. *Mail Transmitted Outside CIG*

Documents to be transmitted outside CIG will be routed in the inter-office chain envelope to the Distribution Section, Central Records Division. (For detailed

RESTRICTED

RESTRICTED

Appendix A (continued 2)

instructions covering the handling and routing of outgoing documents see Part III, Section 2, "Outgoing", of this Appendix.)

d. *Transmitting CONFIDENTIAL or SECRET Documents*

The CIG inter-office chain envelope, when used to transmit CONFIDENTIAL or SECRET documents, will be sealed with one CIG gummed label and the initial of the sealer will be entered in an appropriate place on the seal. These seals may also be obtained from Central Records Division. Under no circumstances should scotch tape be used to seal the inter-office chain envelope.

e. *Transmitting Unclassified or Restricted Documents*

The CIG inter-office chain envelope, when used to transmit only unclassified or Restricted material, need not be sealed in any manner, but the envelope flap should be pushed inside.

f. *Inter-Office Chain Envelope Numbering and Receiving Systems*

Each Office Message Center and each designated pick-up and delivery point within an office will initiate its own numbering series for inter-office chain envelopes, the contents of which are classified SECRET or CONFIDENTIAL. This number will consist of the month expressed in number and the next unused consecutive number, e.g., if the first envelope is dispatched in June, the number would be 6-1; if the tenth envelope is dispatched in July, the number would be 7-10. Since the second number is the identifying envelope number, it would continue in numerical sequence until the end of the calendar year. Thus, if 320 envelopes containing SECRET or CONFIDENTIAL documents have been dispatched as of December 31, the last one would be numbered 12-320. At the beginning of the next calendar year, a new series would be initiated, the first envelope in January of the new year being numbered 1-1. This office envelope number will be placed in the office of dispatch column, before the name in the "From" column. The number appearing on the envelope will also be placed on the attached Receipt Form 35-16.

Receipt Form 35-16 to be attached to inter-office envelopes containing SECRET or CONFIDENTIAL documents will be prepared in the CIG receipt book in duplicate. Receipt Form 35-16 is in triplicate in the receipt book; however, only two copies are to be used and no attention is to be paid to the colors of the copies used. The third copy has a special use in isolated circumstances. The original copy of the receipt will be stapled to the envelope. The preparing office will retain the carbon copy of the receipt for its records. This copy will be signed by the Messenger or Courier who picks up the chain envelope. The number appearing both on the Receipt Form 35-16 and the inter-office chain envelope will be noted in the office log opposite the individual papers transmitted in the inter-office chain envelope. This will provide a record of the documents in any one envelope.

g. *Bulky Documents (Classified)*

Classified documents which, because of bulk, cannot be put in the inter-office chain envelope, will be wrapped in a satisfactory manner, taped with CIG gummed seals, and forwarded in exactly the same manner as an inter-office chain envelope.

3. OPERATION OF COURIER AND MESSENGER SYSTEM

a. *Courier Pick-Up and Delivery*

Central Records Division, Services Branch, will provide offices with pick-up and delivery Courier Service from and to appropriate points located in different build-

RESTRICTED

RESTRICTED

Appendix A
(continued 3)

ings. An inter-office chain envelope containing SECRET or CONFIDENTIAL documents, after being signed for by a Regular Courier on Receipt Form 35-16, will be delivered to the appropriate building and Office Message Center. The appropriate individual in the receiving Office Message Center will remove and sign the original copy of Receipt Form 35-16 attached to the chain envelope and return receipt to Courier. The Central Mail Room will maintain a file of all completed receipts for location purposes. The Courier transmittal of a Restricted or unclassified document to a location in another building is accomplished in the chain envelope without regard to the use of Receipt Form 35-16.

b. *Messenger Pick-Up and Delivery*

Central Records Division, Services Branch, will provide offices with pick-up and delivery messenger service from and to appropriate points within the same building. The delivery of a chain envelope to any office located in another building will be made by Regular Courier as indicated above.

II CIG MESSENGER AND COURIER SERVICES

1. The Central Records Division, Services Branch, will provide each Office and Staff Section of CIG with Messenger and Courier service as follows:

a. *TOP SECRET Couriers*

TOP SECRET Couriers will be used to transmit TOP SECRET documents between individuals and buildings of CIG and between CIG and outside agency.

b. *Regular Couriers*

Regular Couriers will be used to transmit documents classified SECRET or below between buildings of CIG and between CIG and an outside agency.

c. *Messengers*

Messengers will be used to transmit documents classified SECRET or below between individuals and offices located in the same building, but will not carry documents between buildings. Certain messengers, however, may be used to transmit unclassified or Restricted documents between CIG and an outside agency.

d. *Operation of Regular Courier and Messenger Service*

See Part I, Section 3 of this Appendix, "Operation of Courier and Messenger System".

III LOGGING AND ROUTING OF ADMINISTRATIVE DOCUMENTS, OTHER THAN CABLES, CLASSIFIED BELOW TOP SECRET

1. INCOMING

a. *The Central Mail Section will:*

(1) Receive, open, and time-stamp each document entering CIG and route each administrative document to the Distribution Section, Central Records Division, Services Branch. (The only exception to this procedure is an incoming pouch document addressed to OSO which, after being properly recorded, will be routed unopened to the Office of Special Operations.)

RESTRICTED

RESTRICTED

Appendix A
(continued 4)

b. *The Distribution Section will:*

- (1) Assign CIG control number.
- (2) Assign file classification number.
- (3) Prepare CIG Form 35-1 in multiple copies, assigning a suspense date

by which time correspondence must be answered; establish a follow-up system on suspense dates.

(4) Prepare a Consolidated Receipt, CIG Form 35-3, for each receiving Office or Staff Section Message Center and insure the proper return of this receipt for filing.

- (5) Route documents to the Office or Staff Message Center.

c. *The Office or Staff Message Center will:*

- (1) Sign and return CIG Form 35-3 to Distribution Section.

(2) Check document against copies of CIG Form 35-1 which are attached to each document.

(3) Withdraw Office Message Center Copy of CIG Form 35-1 and indicate thereon the particular office subdivision to which the document will be routed.

(4) File CIG Form 35-1 by the CIG control number appearing in the upper left-hand corner of the Form.

- (5) Route document to appropriate Receiving Office.

d. *The Receiving Office will:*

(1) Record document in any appropriate log which will enable that office to account for all documents received by it for action or as a matter of interest.

(2) Return document to Central Files Unit, Distribution Section, for permanent filing after it has served its purpose.

(3) If the document must be retained permanently in the receiving office, remove the copy of CIG Form 35-1 attached to it, note the name of the office of retention thereon, and return it to Distribution Section.

2. OUTGOING

a. *The originating office will:*

- (1) Check document and envelopes for correct preparation.

- (2) Address envelopes.

(3) Insure that a receipt (CIG Form 38-15) has been prepared and is attached to all documents classified SECRET. In the case of documents classified CONFIDENTIAL, Receipt Form 38-15 need not be prepared unless the sender deems it necessary.

(4) Insure that a copy of the document is attached to be withdrawn by Distribution Section and forwarded to Central Files Unit for permanent record. The Central Files copy will have attached to it, when circumstances require, a memorandum for record, or all buck slips, inter-office memoranda, and notes which have preceded the preparation of the document.

(5) Attach a CIG Form 35-11 if a special method of dispatch is desired, i.e., "Air Mail," "Registered," "Special Delivery," "Pouch," etc.

(6) Record the document in the office of origin log and dispatch it to the Office or Staff Message Center in accordance with inter-office chain envelope procedure.

RESTRICTED

RESTRICTED

Appendix A
(continued 5)

b. *The Office or Staff Message Center will:*

- (1) Check to see that an adequate number of copies of the outgoing document has been prepared.
- (2) Insure the adequacy of the memorandum for record on the Central Files copy of the document.
- (3) Check to see that adequate envelopes and receipts have been prepared for use of Distribution Section.
- (4) Assign each document a number preceded by the authorized abbreviation or symbol for the Office or Staff Section. This number will be placed above the return address on the outside envelope.
- (5) Record the document in appropriate log and forward document to Distribution Section in the inter-office chain envelope.
- (6) Get in touch with Distribution Section to determine the cause of delay if a copy of CIG Form 35-1 for each outgoing document has not been received within twenty-four hours after its release.

c. *The Distribution Section will:*

- (1) Check the document to see that it is properly prepared.
- (2) Assign a CIG control number.
- (3) Assign a file classification number and indicate cross-references.
- (4) Prepare CIG Form 35-1.
- (5) Forward to Office or Staff Message Center one copy of CIG Form 35-1 as assurance that the document has been dispatched.
- (6) Forward the document after it has been properly recorded and sealed to the Central Mail Section for actual dispatch.

d. *The Central Mail Section will:*

- (1) Determine from notations on CIG Form 35-11, if attached, what special handling has been requested for the document, and handle in that manner if possible.
- (2) Prepare and maintain all records and receipts for envelopes of classified documents.
- (3) Effect delivery of document to proper transmitting agency.

e. *Sealed Documents*

If for security reasons outgoing documents are to be sealed in the office of origin and the contents are not to be seen by processing personnel, the originating office will:

- (1) Seal the envelopes, placing on the outside envelope a number, preceded by the authorized office abbreviation or symbol, for the use of Central Mail Section in recording the envelope.
- (2) Attach Form 35-11 indicating whether document is to travel through classified or unclassified channels and any special handling requested.
- (3) Dispatch to Central Mail Section via Office Message Center.

f. *Pouch Documents*

Documents to be dispatched by pouch from CIG to destinations outside the District of Columbia through Courier or similar service will be processed in the same manner as any other outgoing document (see Part III, Section 2 of this Appendix).

RESTRICTED

RESTRICTED

Appendix A
(continued 6)

Documents from OSO intended for dispatch to locations outside the District of Columbia will be delivered already wrapped to the Central Mail Section, for recording and forwarding through proper transmitting channels.

3. INTER-OFFICE

a. *Office or Staff Message Center Procedures*

It is the responsibility of the Office or Staff Message Center to keep adequate records of all inter-office handling and routing of documents. Channeling of documents through Central Records Division will not be required in inter-office exchanges. The system for recording inter-office documents will be developed to fit the needs of each office, the only requirements being that, at all times, the Office or Staff Message Center will be able to account for the disposition of both incoming and outgoing documents and appropriate security precautions are observed. The log used for recording outgoing documents may also be used for recording all types of inter-office documents.

b. *Inter-Office Transmittal of Administrative Documents*

Administrative documents traveling between offices will be forwarded through the Messenger and Courier System in chain envelopes, except TOP SECRET which will be handled either by TOP SECRET Courier or Assistant TOP SECRET Control Officer.

IV LOGGING AND ROUTING OF INTELLIGENCE INFORMATION, OTHER THAN CABLES, CLASSIFIED BELOW TOP SECRET

1. INCOMING

a. *The Central Mail Section will:*

(1) Open and route all intelligence information received in CIG to the Information Distribution Section, Central Records Division, Services Branch. The only exception to this procedure is incoming pouch material for OSO which, after being properly recorded, will be routed unopened to the Office of Special Operations where it will be acknowledged by signed receipt.

b. *The Information Distribution Section will:*

- (1) Assign a CIG control number.
- (2) Assign a file classification number.
- (3) Record the document on CIG Form 35-2.

(4) Deliver each document to the proper representative of the Reading Center, OCD, where the distribution to be accorded the document will be determined.

(5) Make necessary records of distribution as indicated by the Reading Center on CIG Form 35-2 and withdraw Central Records Division copies of such forms.

(6) In the case of ORE, attach three copies of CIG Form 35-2 to copies of reports going to that office.

(7) Prepare Consolidated Receipt (CIG Form 35-3) for all documents and insure the proper return of this Receipt from the office of address.

(8) Dispatch each document to appropriate Office or Staff Message Center.

c. *The Office or Staff Message Center will:*

(1) Check documents against enclosed Consolidated Receipt (CIG Form 35-3) which it will sign and return to Information Distribution Section.

RESTRICTED

RESTRICTED

Appendix A
(continued 7)

- (2) Record Receipt of documents in an appropriate log.
- (3) In the case of ORE, check the documents against the copies of CIG Form 35-2 attached to each document.
- (4) In the case of ORE, withdraw the three Message Center copies of CIG Form 35-2 and indicate thereon the particular subdivision of ORE to which a document is to be routed. The three copies of CIG Form 35-2 will then be filed as follows: one by CIG control number, one by source, and the remaining one by subject.
- (5) Dispatch documents to receiving offices and record disposition in an appropriate log.

d. *The Receiving Office will:*

- (1) Record receipt and disposition of documents in an appropriate log.
- (2) In the case of ORE, maintain record of documents on Form 35-2 supplied the receiving office by ORE Message Center.

2. OUTGOING

At the present time, outgoing intelligence information is processed by the Information Distribution Section, Central Records Division.

3. INTER-OFFICE

Intelligence information documents traveling between offices will be processed in the same manner as administrative material, i.e., through the Messenger and Courier system in chain envelopes. Complete records will be maintained in dispatching and receiving offices.

V PROCESSING OF TOP SECRET DOCUMENTS

1. GENERAL INFORMATION

a. *Transmittal of TOP SECRET Documents between Offices and Divisions of CIG*

Transmittal of TOP SECRET documents between Offices and Executive Staff Sections will be accomplished by a TOP SECRET Courier, e.g., from ORE to OO; from Services Branch to Finance Branch. It is permissible *within* CIG, however, for one Assistant TOP SECRET Control Officer to deliver a TOP SECRET document to another Assistant TOP SECRET Control Officer, the necessary receipt being obtained, provided Central Records Division, Services Branch, is informed of such change of responsibility.

b. *Transmittal of TOP SECRET Documents between Units*

Transmittal of TOP SECRET documents between units of an Office or Executive Staff section will be effected by the Assistant TOP SECRET Control Officer of the Office or Staff Section concerned. When an Office or Staff has personnel in several different buildings, it is permissible to request a TOP SECRET Courier to effect deliveries between buildings.

c. *TOP SECRET Signature Record and Cover Sheet (CIG Form 38-13)*

The TOP SECRET Signature Record and Cover Sheet (CIG Form 38-13) will not be removed from a TOP SECRET document until the document is destroyed, downgraded, or dispatched outside of CIG. However, when a document is so treated,

RESTRICTED

RESTRICTED

Appendix A (continued 8)

the particular disposition is noted on the TOP SECRET Signature Record and Cover Sheet and the sheet is sent to Special Distribution Section to be filed. This sheet will serve as a cover to a TOP SECRET document and will provide a record of all individuals who have had access to the document. Each individual who uses or processes a TOP SECRET document, will affix his signature to the sheet and indicate thereon date and time of receipt. When releasing material to another authorized individual, he will affix his initials and indicate date and time of release.

2. INCOMING

a. *Special Distribution Procedures*

All TOP SECRET documents, administrative or intelligence (except cables, and documents pertaining solely to the Office of Special Operations), shall be delivered initially to Special Distribution Section, Central Records Division, Services Branch. (Any member of CIG who receives a TOP SECRET document from an outside source in a manner which has by-passed Special Distribution Section will report the fact to Special Distribution Section as soon as possible in order that the document may be properly processed.)

b. *The Special Distribution Section will:*

- (1) Assign CIG control number to each document.
- (2) Assign CIG file classification number.
- (3) Log document.
- (4) Staple a TOP SECRET Signature Record and Cover Sheet (CIG Form 38-13) to document.

(5) In the case of administrative documents, determine the routing to be given each document and make appropriate notations on all records and CIG Form 38-13.

(6) In the case of intelligence information, pass the document to a specifically designated member of the Reading Center, OCD, for determination of distribution.

(7) Make a record of the recommended distribution after the document returns from the Reading Center.

- (8) Prepare a Document Receipt (CIG Form 38-16) for each document.
- (9) Route each document to appropriate Office or Staff Section Message Center.

c. *The Office or Staff Section Message Center will:*

(1) Check document against the Document Receipt Form 38-16 which it will sign and return to Special Distribution Section through the Messenger-Courier system.

(2) Record document in a TOP SECRET log. (A suggested log sheet that may be used is CIG Form 38-14.)

(3) Insure that the Signature Record and Cover Sheet on each document is initialed by everyone examining or handling the document within the Message Center.

(4) Request its Assistant TOP SECRET Control Officer to deliver the TOP SECRET document to the receiving office where the document will be acknowledged by signature in the Message Center TOP SECRET log. An optional procedure will be to have the document delivered to the receiving office by a TOP SECRET Courier, in which

RESTRICTED

RESTRICTED

Appendix A (continued 9)

case the Courier will sign for the envelope containing the document and make delivery to the Receiving Office where Document Receipt Form 38-16 will be signed and returned to the Office Message Center.

d. *The Receiving Office will:*

(1) Sign for the document in the Message Center TOP SECRET log if delivered by Assistant TOP SECRET Control Officer; or, sign and return Document Receipt Form 38-16 if delivered by TOP SECRET Courier.

(2) Enter the document in a TOP SECRET log.

(3) Insure that each person handling or examining the document enters his name, initials, and dates of handling on the TOP SECRET Signature Record and Cover Sheet.

(4) In case it receives permission to downgrade or destroy the document, remove the Signature Record and Cover Sheet, note the particular action or disposition at the bottom of the Sheet, and forward the Sheet through the Office or Staff Section Message Center to Special Distribution Section, Central Records Division, Services Branch.

(5) If the document is intelligence material, forward it to the Reference Branch, ORE, for permanent retention in the TOP SECRET files of that office. Here the Signature Record and Cover Sheet will be removed after notation has been made thereon that the document has been filed, and the Sheet returned to Special Distribution Section through the Office or Staff Section Message Center.

(6) If a document is of special administrative nature, forward it with Signature Record and Cover Sheet still attached to Special Distribution Section for file.

3. OUTGOING

a. *General*

A TOP SECRET document prepared in an office will be processed in the following manner:

b. *The originating office will:*

(1) Check to see that it conforms to CIG correspondence and/or security regulations.

(2) Insure that security classification has been properly affixed with appropriate authority indicated for the classification.

(3) Prepare Receipt Form 38-15 to be attached to the document.

(4) Prepare two envelopes, the smaller to be stamped with the TOP SECRET classification.

(5) Attach a TOP SECRET Signature Record and Cover Sheet, Form 38-13, to the document.

(6) Assign to the document a number preceded by the authorized initials or symbols of the preparing office and enter in the TOP SECRET log.

(7) Deliver the document to the Office or Staff Message Center and receive a signature receipt in the TOP SECRET log of the originating office. If the originating office is in a different building from that of the Office or Staff Message Center, a TOP SECRET Courier should be called and a sealed envelope given him containing the document, the Receipt Form 38-15, the prepared envelopes, the Signature Record and Cover Sheet, and a Document Receipt (Form 38-16), the latter for execu-

RESTRICTED

RESTRICTED

Appendix A
(continued 10)

tion by the Assistant TOP SECRET Control Officer of the Office or Staff Section Message Center. The originating office will require a receipt from the TOP SECRET Courier for the sealed envelope and its contents.

c. *The Assistant TOP SECRET Control Officer will:*

(1) Sign for the document in the TOP SECRET log of the originating office, or open the sealed envelope delivered by the TOP SECRET Courier and execute the CIG Document Receipt (Form 38-16) which will be returned to the originating office.

(2) Record the document in the TOP SECRET log of the Office or Staff Message Center. Special care must be taken to insure that each person handling or processing the document executes the attached Signature Record and Cover Sheet.

(3) Check to see whether the document has been correctly prepared, properly signed, and receipt and envelopes attached for use of Special Distribution Section, Central Records Division.

(4) Deliver the document to the Special Distribution Section and receive in his TOP SECRET log a signature receipt therefor; or, as an optional procedure, enclose the document (to which will be attached a Document Receipt, Form 38-16) in a sealed envelope and call a TOP SECRET Courier. The TOP SECRET Courier will sign a receipt for the envelope and its contents and make delivery to Special Distribution Section.

d. *The Special Distribution Section will:*

(1) Sign for the document in the TOP SECRET log of the Assistant TOP SECRET Control Officer making the delivery; or, if the material has been delivered by TOP SECRET Courier, sign the envelope receipt and the enclosed Document Receipt (Form 38-16), the former to be retained by the Courier and the latter to be returned to the appropriate Office or Staff Section Message Center immediately.

(2) Record the document on the standard record slip (Form 35-1), one copy of which will be returned to the Message Center of origin.

(3) Insure that a Receipt Form 38-15 has been prepared, as well as the envelopes necessary for the dispatch of the document.

(4) Insure that the Signature Record and Cover Sheet has been properly executed by personnel in Special Distribution Section who have handled or processed the TOP SECRET document.

(5) Remove the Signature Record and Cover Sheet noting thereon the disposition which is to be made of the document.

(6) Remove and file the Central Files Unit copy of the document.

(7) After preparing necessary envelope records, determine the correct channel for the transmittal of the document and deliver it thereto.

4. INTER-OFFICE

a. *The originating office will:*

(1) After checking a document for correctness, security classification, and authorization for such classification, make proper record in the office TOP SECRET log.

(2) Attach a TOP SECRET Signature Record and Cover Sheet, Form 38-13, to the document and indicate on the second line of the Cover Sheet the name of the first person to whom the document will be sent.

RESTRICTED

RESTRICTED

Appendix A
(continued 11)

(3) Deliver the document to the Assistant TOP SECRET Control Officer of the Office or Staff Message Center and secure his signature in a TOP SECRET log; or, as an optional procedure, enclose the document (to which will be attached a Document Receipt, Form 38-16) in a sealed envelope and call a TOP SECRET Courier. The TOP SECRET Courier will sign a receipt for the envelope and its contents and make delivery to the Assistant TOP SECRET Control Officer of the Office or Staff Message Center.

b. *The Office or Staff Section Message Center will:*

(1) Sign for the document in the TOP SECRET log of the originating office; or, if delivered by TOP SECRET Courier, sign the envelope receipt and enclosed Document Receipt, Form 38-16, the former to be retained by the Courier and the latter to be returned to the originating office.

(2) Enter the TOP SECRET document in the Message Center TOP SECRET log.

(3) Insure that each person who handles or processes the document executes the Signature Record and Cover Sheet.

(4) Deliver the document by Assistant TOP SECRET Control Officer to the receiving Office or Staff Section Message Center and have the Assistant TOP SECRET Control Officer of that Office sign for the document in the originating Office or Staff Section Message Center log; or, will send the document in an envelope covered by a receipt by TOP SECRET Courier to the receiving Message Center, insuring that a Document Receipt, Form 38-16, is enclosed for execution and return by the Assistant TOP SECRET Control Officer of the receiving Message Center.

c. *The Receiving Message Center will:*

(1) Sign for the document in the TOP SECRET log of the originating Message Center; or, sign the envelope receipt and enclosed Document Receipt, Form 38-16, the former to be retained by the TOP SECRET Courier and the latter to be returned to the originating Message Center.

(2) Record the document in its TOP SECRET log.

(3) Insure that each person who handles or processes the document within the Message Center executes the Signature Record and Cover Sheet.

(4) Deliver the document to the receiving office by Assistant TOP SECRET Control Officer who will obtain a signature receipt in the TOP SECRET log of the Message Center. If the receiving office is in another building, it will be necessary to deliver the document by TOP SECRET Courier, the customary receipt being obtained. Upon receipt of the document, the receiving office will sign Document Receipt, Form 38-16, and return it to the Message Center.

d. *The Receiving Office will:*

(1) Sign the TOP SECRET log of the Assistant TOP SECRET Control Officer; or, if the document has been delivered by TOP SECRET Courier, sign the envelope receipt and the Document Receipt (Form 38-16), the former to be retained by the TOP SECRET Courier and the latter to be returned to the Message Center.

(2) Record the document in its TOP SECRET log.

(3) Insure that each person who uses or handles the document executes the TOP SECRET Signature Record and Cover Sheet.

RESTRICTED

RESTRICTED

Appendix A
(continued 12)

5. OUTGOING TOP SECRET INTELLIGENCE

a. *General Instruction*

All CIG-produced TOP SECRET intelligence documents will be distributed by the Special Distribution Section, Central Records Division, Services Branch. Upon receipt of such documents for distribution, Special Distribution Section will supply the originating office with a Consolidated Receipt (CIG Form 35-3) for all copies. It will then distribute the documents in accordance with existing security regulations.

RESTRICTED

RESTRICTED